Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN04/001516

International filing date: 24 December 2004 (24.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200310121080.8
Filing date: 24 December 2003 (24.12.2003)

Date of receipt at the International Bureau: 24 February 2005 (24.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/CN2004/001516

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　　请　　日：　2003.12.24

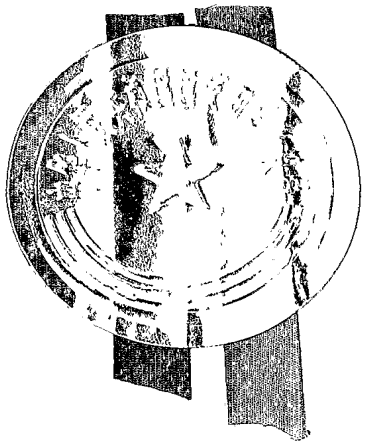
申　　请　　号：　200310121080.8

申 请 类 别：　发明

发明创造名称：　实现网络地址转换穿越的方法及其系统

申　　请　　人：　华为技术有限公司

发明人或设计人：　袁莉、严军



中华人民共和国
国家知识产权局局长　王景川

2005 年 1 月 13 日

权 利 要 求 书

1. 一种实现网络地址转换穿越的方法，其特征在于包含以下步骤：

A 当网络地址转换服务器或防火墙以外的代理服务器收到来自第一网络内分组用户终端的呼叫信令时，对该呼叫信令的报文负载信息进行解析，记录该报文负载信息中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载信息中的呼叫信令地址和端口修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载信息中的媒体流实时传输协议和实时传输控制协议地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口；

B 所述代理服务器将修改后的所述呼叫信令发送到分组语音信令处理设备或业务处理设备；

C 当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载信息中回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载信息所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为所述被记录的媒体流实时传输协议和实时传输控制协议地址和端口；

D 所述代理服务器将修改后的所述回应信令发向所述第一网络内分组用户终端。

2. 根据权利要求 1 所述的实现网络地址转换穿越的方法，其特征在于，还包含以下步骤：

所述步骤 A 执行以后，所述代理服务器定期向所述第一网络内分组用户终端发起报文，刷新所述网络地址转换服务器或防火墙上的信令地址映射关系。

3. 根据权利要求 1 所述的实现网络地址转换穿越的方法，其特征在于，所述分组语音信令处理设备或业务处理设备是软交换设备或 IP 语音网守设备。

4. 根据权利要求 1 所述的实现网络地址转换穿越的方法，其特征在于，还进一步包含以下步骤：

当所述代理服务器收到来自所述第一网络内分组用户终端的呼叫信令时，记录该呼叫信令的报文 IP 头地址和端口，并将其修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口；

当所述代理服务器收到发向所述第一网络内分组用户终端的呼叫信令时，将该呼叫信令的报文 IP 头地址和端口修改为所述被记录的呼叫信令的报文 IP 头地址和端口。

5. 一种实现网络地址转换穿越的系统，其特征在于，包含分组用户终端、网络地址转换服务器或防火墙、代理服务器和软交换设备；

所述分组用户终端位于第一网络内，用于发起和接收业务；

所述网络地址转换服务器或防火墙用于为所述分组用户终端提供接入第二网络的服务，为所述分组用户终端和所述代理服务器相互转发报文；

所述代理服务器在第二网络内，用于接收源自所述分组用户终端的呼叫信令，对该呼叫信令的报文负载信息进行解析，记录该报文负载中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载中的呼叫信令地址修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载中的媒体流实时传输协议和实时传输控制协议地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口，然后将修改后的所述呼叫信令发送到所述软交换设备；此外，当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载中

回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为所述被记录的媒体流实时传输协议和实时传输控制协议地址和端口，然后将修改后的所述回应信令发向所述第一网络内分组用户终端；

所述软交换设备用于提供综合业务和呼叫控制，在收到发送给所述分组用户终端的信令时转发给所述代理服务器。

6. 根据权利要求 5 所述的实现网络地址转换穿越的系统，其特征在于，所述分组用户终端是使用 H.323 协议、或会话初始化协议、或媒体网关控制协议、或 H.248 协议进行音频和视频通信的用户终端。

7. 根据权利要求 5 所述的实现网络地址转换穿越的系统，其特征在于，所述代理服务器还用于按照流量计费。

8. 根据权利要求 5 所述的实现网络地址转换穿越的系统，其特征在于，所述代理服务器还用于用户的接入控制、带宽管理，对媒体流的服务质量标记、虚拟专用网标记和信息进行加密。

9. 根据权利要求 5 所述的实现网络地址转换穿越的系统，其特征在于，所述代理服务器还用于多个第一网络和第二网络地址对的设置，同时实现对多个网络地址转换服务器或防火墙的穿越。

10. 根据权利要求 5 所述的实现网络地址转换穿越的系统，其特征在于，对于媒体流的交互，所述代理服务器采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项。

说　明　书

实现网络地址转换穿越的方法及其系统

技术领域

本发明涉及下一代网络中的通信系统和方法，特别涉及下一代网络中流媒体穿越网络地址转换/防火墙的系统和方法。

背景技术

下一代网络（Next Generation Network，简称“NGN”）是电信史的一块里程碑，它标志着新一代电信网络时代的到来。从发展的角度来看，NGN是从传统的以电路交换为主的公用电话交换网（Public Switched Telephone Network，简称“PSTN”）中逐渐迈出了向以分组交换为主的步伐，它承载了原有 PSTN 网络的所有业务，把大量的数据传输卸载到网间互联协议（Internet Protocol，简称“IP”）网络中以减轻PSTN网络的重荷，又以IP技术的新特性增加和增强了许多新老业务。从这个意义上讲，NGN是基于时分多路复用（Time Division Multiplexing，简称“TDM”）的PSTN语音网络和基于网间互联协议/异步传输模式（IP/ATM）的分组网络融合的产物，它使得在新一代网络上语音、视频、数据等综合业务成为了可能。目前，NGN成为了研究的热点。

NGN在功能上可分为四个层次：接入和传输层、媒体传送层、控制层、网络服务层。软交换（SoftSwitch）为NGN提供具有实时性要求的业务的呼叫控制和连接控制功能，是NGN呼叫与控制的核心。软交换构件（SoftX）为 NGN 的网络控制层的关键构件，是提供综合业务和呼叫控制的设备。其主要作用包括：呼叫控制、信令网关、网关控制、综合业务、增强业务等。

随着NGN网络逐步从实验走向商用，NGN用户的接入问题越来越成为一个严重的问题。由于 NGN 是一个基于分组网承载的网络，接入用户都是

通过 IP 地址来寻址，而当前的网络由于 IP 地址紧缺以及安全等各原因，大量的企业网和驻地网基本上都采用了私有 IP 地址通过出口的网络地址转换/防火墙（NAT/FW）接入公网。

然而，目前 NGN 网络中，在 IP 上承载诸如 H.323、会话初始协议（Session Initiationl Protocol，简称“SIP”）、网关控制协议（Media Gateway Control Protocol，简称“MGCP”）、H.248 等语音和视频协议时，由于报文的负载中有与报头不一样的地址，使得这些协议的控制通道/媒体通道难以穿越传统的 NAT/FW 设备与公网进行互通。其具体原因可通过对 NAT/FW 的分析得知：

防火墙，即 FW，用于限制数据包无限制的进入网络内。一般是设定一些包过滤原则，防火墙通过检查数据包的源地址、目标地址、源端口、目标端口和协议来判断数据包是否符合过滤原则，符合的才可以通过防火墙。实际应用时通常将一些需要外界访问的服务器，如 Web 服务器等放在这个区域内，防火墙配置成让所有发往这些服务器的对应端口的数据可以通过。在进行多媒体通信时，即使防火墙可以让最初建立呼叫的发往固定端口的数据包进入，由于音/视频通信需要通过动态端口分配来建立发送和接收数据的通道，其范围较大且无法事先预知内部终端的 IP 地址和端口信息，防火墙不可能不顾局域网的安全，开放这么大的包过滤范围。

另一方面，再从 NAT 考察有关原因：

NAT 用于隐藏局域网 IP、保护局域网内主机不受外界攻击。由于局域网内的地址无法在公网上进行路由寻址，当数据包的目标地址是 LAN 内地址时，数据包只能被丢弃掉。在进行多媒体通信时，如果 H.323 被呼叫方的地址是局域网地址，则呼叫的数据包根本无法到达局域网内终端。当呼叫从局域网内向外发起时，呼叫方的 IP 地址(局域网 IP)和端口信息会加载在数据包的负荷当中，接收端接收到数据包后，根据数据包负载中的源 IP 地址和端口

发送音频、视频流，当这个 IP 是一个无法进行路由寻址的 IP 时，Internet 上的路由器只能把这些数据丢掉，表面上看起来呼叫已经连接起来了，但实际上在 NAT 内的终端是无法接收到外面终端的音频和视频的。另外 NAT 还通过网络地址端口转换使局域网内的多个终端能够共享较少数量的公网 IP 地址。如在局域网内的某个终端执行某个应用时，将其局域网 IP 地址和端口映射成网关的外网 IP 和端口。在多媒体通信时，只有多媒体流通道是从内向外建立时，NAT 设备才可以建立对应的端口映射关系，传送到网关的外网 IP 上的多媒体流才可正确地传送到局域网的终端。如果多媒体流通道是从外向内建立的，则 NAT 设备无法建立映射关系，多媒体流的传送会失败。再有，如果这些通道采用的是超时的机制维持，如果在超时时间内该通道没有数据传送，这个映射关系就会被取消掉，在多媒体通信时，如果需要有很长时间停止通道上多媒体数据传送时，需要采取一定的措施来维持通道的建立。

上面详细分析了音频、视频业务无法通过 NAT/FW 的原因。然而，NGN 网络最大的好处之一就是能为用户提供丰富的业务，特别是为企业用户提供语音、数据、视频融合的业务，因此上面所提到问题的解决就更加的迫切，成为目前 NGN 网络业务开展最大的障碍。另一方面，宽带接入网络由于大多不属于运营商网络，运营商无法对其进行统一规划，使得接入网络的 IP 地址问题，业务质量保证（Quality of Service，简称“QoS”）和安全保证问题，实时会话业务和数据业务的区分等问题难以得到解决，成为困扰运营商的重要方面。

目前业界现有的解决方法有应用层网关方式（Application Layer Gateway，简称“ALG”）、中间盒通讯方式（Middlebox Communication，简称“MIDCOM”）、用户数据报协议（UDP）对 NAT 的简单穿越方式（Simple Traversal of UDP Through Network Address Translators，简称“STUN”）、通过中继（中继）方式穿越 NAT 方式（Traversal Using 中继 NAT，简称“TURN”）。

下面简单说明上述各种现有技术的内容。

ALG 方式

普通 NAT 是通过修改用户数据报协议（User Datagram Protocol，简称“UDP”）或传输控制协议（Transfer Control Protocol，简称“TCP”）报文头部地址信息实现地址的转换，但部分承载于 TCP/UDP 的应用，例如多媒体会话、文件共享、游戏等“端到端”的应用，在 TCP/UDP 负载中也需带地址信息。一般的方法，应用程序在负载中填写的是其自身地址，此地址信息在通过 NAT 时被修改为 NAT 上对外的地址，即我们常说的 ALG 方式。

ALG 功能目前主要驻留在一些 NAT/Firewall 设备中，要求这些设备本身具备应用识别的智能.同时每增加一种新的应用都将需要对 NAT/Firewall 进行升级。

对 NGN 业务应用，ALG 需要支持 IP 语音和诸如 H323、SIP、MGCP/H248 等视频协议的识别和对 NAT/Firewall 的控制，以使 NGN 业务顺利穿越。

ALG 的关键点为：企业网/驻地网内部终端设备能穿透 NAT/ALG 注册到公网 SoftX 上，通过 SoftX 进行协议解析和呼叫处理。公网 SoftX 和企业网终端通过 SIP/H323/MGCP/H248 协议互通，NAT/ALG 需要识别 SIP/H323/MGCP/H248 协议信令并建立媒体流通道，以支持媒体流顺利穿越 NAT/FW。

ALG 是支持 NGN 应用一种最简单的方式，但由于网络实际情况是已部署了大量的不支持 NGN 业务应用的 NAT/FW 设备，另外，它还存在一些不足（将在第二部分详细说明）所以难以推广。

MIDCOM 方式

MIDCOM 与 ALG 不同，MIDCOM 的框架结构是采用可信的第三方 MIDCOM 代理（MIDCOM Agent）对中间盒（Middlebox） 进行控制的机制，

应用业务识别的智能也由 Middlebox 转移到外部的 MIDCOM Agent 上，因此应用协议对 Middlebox 是透明的 。

由于应用业务识别的智能从 Middlebox 移到外部的 MIDCOM Agent 上，根据 MIDCOM 的架构，在不需要更改 Middlebox 基本特性的基础上，通过对 MIDCOM Agent 的升级就可以支持更多的新业务，这是相对 ALG 方式的一个很大的优势。

在 NGN 业务实际应用中，Middlebox 功能可驻留在 NAT/FW，MIDCOM Agent 功能可驻留在 SoftX。通过软交换设备 中的 MIDCOM Agent 对 IP 语音和诸如 H323、SIP、MGCP/H248 等视频协议的识别和对 NAT/ FW 的控制，它可以作为 NGN 业务穿越 NAT/FW 的一个解决方案。

MIDCOM 方式的关键点为：公网 SoftX 通过 MIDCOM 协议对私网边缘的 NAT/FW 设备进行控制，SoftX 识别主被叫侧的 SIP/H323/MGCP/H248 协议，如主被叫侧均为局内的私网用户，SoftX 需要通过 MIDCOM 协议控制主被叫两侧的 NAT/FW，在 NAT/FW 上创建了媒体流通道后，媒体流可顺利穿越 NAT/FW。

由于软交换设备SoftX上已实现了对SIP/H323/MGCP/H248协议的识别，只需在 NAT/FW 设备上增加 MIDCOM 协议即可，而且以后新的应用业务识别随着软交换的支持而支持，因此这种方案是一种比较有前途的解决方案，但现有的 NAT/FW 设备需升级支持 MIDCOM 协议。

STUN 方式

解决 NGN NAT 问题的另一思路是，私网接入用户通过某种机制预先得到其地址对应在出口 NAT 上的对外地址，然后在报文负载中所描述的地址信息就直接填写出口 NAT 上的对外地址，而不是私网内用户的私有 IP 地址，这样报文负载中的内容在经过 NAT 时就无需被修改了，只需按普通 NAT 流程转换报文头的 IP 地址即可，负载中的 IP 地址信息和报文头地址信息又是

一致的。STUN 协议就是基于此思路来解决应用层地址的转换问题。

用户的应用程序,作为 STUN 客户端(STUN CLIENT)向 NAT 外的 STUN 服务器（STUN SERVER）通过 UDP 发送请求 STUN 消息，STUN SERVER 收到请求消息，产生响应消息，响应消息中携带请求消息的源端口，即 STUN CLIENT 在 NAT 上对应的外部端口。然后响应消息通过 NAT 发送给 STUN CLIENT，STUN CLIENT 通过响应消息体中的内容得知其在 NAT 上对应的外部地址，并且将其填入以后呼叫协议的 UDP 负载中，告知对端，本端的实时传输协议（RealTime Transfer Protocol ，简称“RTP”）接收地址和端口号为 NAT 外的地址和端口号。由于通过 STUN 协议已在 NAT 上预先建立媒体流的 NAT 映射表项，故媒体流可顺利穿越 NAT。

STUN 协议最大的优点是无需现有 NAT/FW 设备做任何改动。由于实际的网络环境中，已有大量的 NAT/FW，并且这些 NAT/FW 并不支持分组语音（Voice over IP，简称“VoIP”）的应用，如果用 MIDCOM 或 NAT/ALG 方式来解决此问题，需要替换现有的 NAT/FW，这是不太容易的。而采用 STUN 方式无需改动 NAT/FW，这是其最大优势，同时 STUN 方式可在多个 NAT 串联的网络环境中使用，但 MIDCOM 方式则无法实现对多级 NAT 的有效控制。

根据 STUN 原理，STUN SERVER 必须放在公网中，可以内嵌在公网 SoftX 中，由于通过 STUN 协议已在 NAT 上预先建立媒体流的 NAT 映射表项，故媒体流可顺利穿越 NAT。

STUN 的局限性在于需要应用程序支持 STUN CLIENT 的功能，即 NGN 的网络终端需具备 STUN CLIENT 功能。同时 STUN 并不适合支持 TCP 连接的穿越，因此不支持 H323 应用协议。另外 STUN 方式还不支持 NGN 业务对防火墙的穿越，同时 STUN 方式不支持对称 NAT 类型的穿越。

TURN 方式

TURN 方式的解决 NAT 问题的思路与 STUN 相似，也是基于私网接入用户通过某种机制预先得到其私有地址对应在公网的地址，然后在报文负载中所描述的地址信息就直接填写该公网地址的方式。不同的是，STUN 方式得到的地址为出口 NAT 上的地址，TURN 方式得到地址为 TURN 服务器（TURN SERVER）上的地址。

TURN 应用模型如图 1 所示，系统由分组用户终端 10、11，NAT/FW20、21，SoftX40、41 以及 TURN SERVER50 组成。它通过分配 TURN Server 的地址和端口作为 TURN 客户端（TURN CLIENT）对外的接受地址和端口，即私网用户发出的报文都要经过 TURN SERVER 进行中继转发。值得指出，这正是 STUN 方式与 TURN 方式区别最大的地方。这种方式应用模型除了具有 STUN 方式的优点外，还解决了 STUN 应用无法穿透对称 NAT（Symmetric NAT）以及防火墙设备的缺陷，即无论企业网/驻地网出口为哪种类型的 NAT/FW，都可以实现 NAT 的穿透，同时 TURN 支持基于 TCP 的应用，如 H323 协议。此外 TURN SERVER 控制分配地址和端口，能分配实时传输协议（RealTime Transfer Protocol ，简称“RTP”）/实时传输控制协议（RealTime Transfer Control Protocol ，简称“RTCP”）地址对作为本端客户的接受地址，其中 RTCP 端口号为 RTP 端口号加 1，从而避免了 STUN 应用模型下出口 NAT 对 RTP/RTCP 地址端口号的任意分配，使得客户端无法收到对端发过来的 RTCP 报文。

TURN 的局限性在于需要终端支持 TURN CLIENT，这一点同 STUN 一样对网络终端有要求。此外，所有报文都必须经过 TURN SERVER 转发，增大了包的延迟和丢包的可能性。

在实际应用中，上述方案存在以下问题：对于 ALG 方式，不但需要对现有的大量 NAT/FW 进行改造以支持 ALG，而且 NAT/FW 此时难以支持业务的变化，还有因为 ALG 不能识别加密后的报文内容，所以必须保证报文

采用明文传送，这使得报文在公网中传送时有很大的安全隐患。

对于 MIDCOM 方式，需要对现有大量的 NAT/FW 进行升级以支持 MIDCOM。作为运营商难以对属于企业的 NAT/FW 进行升级和管理。

对于 TURN 方式，需要 NGN 的网络终端具备 TURN Client 功能，此外如果多媒体终端的信令收端口和发端口不一致，RTP/RTCP 的收端口和发端口不一致则可能造成无法穿越 NAT 的问题。

对于 STUN 方式，除了具有与 TURN 一样的问题，即需要网络终端支持和会因端口配置不一致而无法穿越 NAT 外，它还有以下问题：不适合支持 TCP 连接穿越和对称 NAT 的穿越。

造成这种情况的主要原因在于，一方面，ALG、MIDCOM、STUN、TURN 方式的实现需要 NAT/FW 或用户终端的支持；另一方面，由于各种方式本身的缺陷，使得它们在面对一些应用无能为力。

发明内容

有鉴于此，本发明的主要目的在于提供一种实现网络地址转换穿越的方法及其系统，使得在任何组网形式下实现穿越时均不需要对现有的 NAT/FW 和用户终端进行改造，并同时解决 QoS、安全以及 NAT 映射表老化的问题。

为实现上述目的，本发明提供了一种实现网络地址转换穿越的方法，包含以下步骤：

A 当网络地址转换服务器或防火墙以外的代理服务器收到来自第一网络内分组用户终端的呼叫信令时，对该呼叫信令的报文负载信息进行解析，记录该报文负载信息中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载信息中的呼叫信令地址和端口修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载信息中的媒体流实时传输协议和实时传输控制协议地址

和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口；

B 所述代理服务器将修改后的所述呼叫信令发送到分组语音信令处理设备或业务处理设备；

C 当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载信息中回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载信息所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为所述被记录的媒体流实时传输协议和实时传输控制协议地址和端口；

D 所述代理服务器将修改后的所述回应信令发向所述第一网络内分组用户终端。

其中，还包含以下步骤：

所述步骤 A 执行以后，所述代理服务器定期向所述第一网络内分组用户终端发起报文，刷新所述网络地址转换服务器或防火墙上的信令地址映射关系。

所述分组语音信令处理设备或业务处理设备是软交换设备或 IP 语音网守设备。

还进一步包含以下步骤：

当所述代理服务器收到来自所述第一网络内分组用户终端的呼叫信令时，记录该呼叫信令的报文 IP 头地址和端口，并将该呼叫信令的报文 IP 头地址和端口修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口；

当所述代理服务器收到发向所述第一网络内分组用户终端的呼叫信令时，将该呼叫信令的报文 IP 头地址和端口修改为所述被记录的呼叫信令的报

文 IP 头地址和端口。

本发明还提供了一种实现网络地址转换穿越的系统，包含分组用户终端、网络地址转换服务器或防火墙、代理服务器和软交换设备；

所述分组用户终端位于第一网络内，用于发起和接收业务；

所述网络地址转换服务器或防火墙用于为所述分组用户终端提供接入第二网络的服务，为所述分组用户终端和所述代理服务器相互转发报文；

所述代理服务器在第二网络内，用于接收源自所述分组用户终端的呼叫信令，对该呼叫信令的报文负载信息进行解析，记录该报文负载中的呼叫信令地址和端口，以及媒体流实时传输协议和实时传输控制协议地址和端口，并且将该报文负载中的呼叫信令地址修改为所述代理服务器为该呼叫分配的在第二网络中的呼叫信令地址和端口，将该报文负载中的媒体流实时传输协议和实时传输控制协议地址和端口修改为所述代理服务器为该媒体流分配的在第二网络中的地址和端口，然后将修改后的所述呼叫信令发送到所述软交换设备；此外，当所述代理服务器收到发向所述第一网络内分组用户终端的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载中回应信令地址和端口修改为所述被记录的呼叫信令地址和端口，将该报文负载所携带的媒体流实时传输协议和实时传输控制协议地址和端口，修改为所述被记录的媒体流实时传输协议和实时传输控制协议地址和端口，然后将修改后的所述回应信令发向所述第一网络内分组用户终端；

所述软交换设备用于提供综合业务和呼叫控制，在收到发送给所述分组用户终端的信令时转发给所述代理服务器。

其中，所述分组用户终端是使用 H.323 协议、或会话初始化协议、或媒体网关控制协议、或 H.248 协议进行音频和视频通信的用户终端。

所述代理服务器还用于按照流量计费。

所述代理服务器还用于用户的接入控制、带宽管理，对媒体流的服务质量标记、虚拟专用网标记和信息进行加密。

所述代理服务器还用于多个第一网络和第二网络地址对的设置，同时实现对多个网络地址转换服务器或防火墙的穿越。

对于媒体流的交互，所述代理服务器采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项。

通过比较可以发现，本发明的技术方案与现有技术的区别在于，本发明通过代理服务器对 NAT/FW 进行穿越，代理服务器不但对报文 IP 头的地址/端口进行转换，而且对报文中携带的信令地址/端口以及 RTP/RTCP 地址/端口也进行转换。

这种技术方案上的区别，带来了较为明显的有益效果，即该方案不需要 NAT/FW 设备进行任何改造；对业务终端没有需求，不需要终端修改；可以实现多层 NAT 和对称 NAT 的穿越；能同时实现对多个企业网/驻地网出口 FW/NAT 的穿越；提供用户的接入控制功能，提供对媒体流的 QoS 标记和信息加密，解决接入网络中实时会话业务的 QoS 保证和安全问题；而且还具有刷新 NAT 映射表和流量计费的功能。

附图说明

图 1 是 TURN 方式下的系统结构图；

图 2 是根据本发明的一个实施例的 FULL PROXY 方式的系统结构图；

图 3 是根据本发明的一个实施例的 FULL PROXY 方式的实现 NAT/FW 穿越的方法流程。

具体实施方式

为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

本发明采用全代理（FULL PROXY）方式，通过对私网内用户呼叫的信令和媒体同时做中继来实现出口 NAT/FW 的穿越，与 TURN 方式的中继相比，有如下区别：

TURN 方式是在 TURN SERVER 与终端通过 TURN 协议交互时分配地址/端口，报文内部的地址信息由终端生成，TURN SERVER 对后续的报文根据分配的地址/端口信息做地址变换后中继转发。而 FULL PROXY 方式是通过对报文进行中继的设备对呼叫协议解析与处理，改写其中携带的 RTP/RTCP 地址信息后转发信令报文，同时根据改写的 RTP/RTCP 地址信息对媒体报文做地址变换后中继转发。

现参照图 2 描述根据本发明的一个实施例的 FULL PROXY 方式的系统结构图。

为突出本发明，图中只标出与本发明有密切关系的部分。如图 2 所示，系统由分组用户终端 10 和 11、NAT/FW20 和 21、代理服务器（PROXY SERVER）30、软交换设备（SoftX）40 和 41 组成。其中，分组用户终端 10、11 分别通过 NAT/FW20、21 跟 PROXY SERVER30 相连；PROXY SERVER30 与 SoftX40、41 相连。图中实线为媒体流，虚线为信令流。

分组用户终端 10、11 是指使用诸如 H.323、会话初始化协议（Session Initation Protocol，简称“SIP”）、媒体网关控制协议（Media Gateway Control Protocol，简称“MGCP”）、H.248 等音频/视频协议通信的用户终端。它们是多媒体业务的发起者和接收者，在私网中，通过分别 NAT/FW20 和 21 接入公网。

NAT/FW20、21 是指实现 NAT 功能和防火墙功能的设备，通常配置在私网接入公网的位置。它一方面用于防止数据包无限制的进入网络内，保护私网内主机不受外界攻击；另一方面通过网络地址端口转换，隐藏私网 IP，使私网内的多个终端能够共享较少数量的公网 IP 地址。如现有技术中所述，

NAT/FW20、21 一般无法让音频/视频流实现穿越。

PROXY SERVER30 类似于 TURN SERVER，放在城域网汇聚层，用于实现 FULL PROXY 的功能，即信令代理以及媒体中继功能。具体功能如下：

PROXY SERVER30 在收到来自分组用户终端 10 的呼叫信令时，对呼叫信令的报文负载中携带的 RTP/RTCP 信息进行解析与处理，记录呼叫信令的报文 IP 头地址/端口，记录报文负载中的呼叫信令地址/端口，记录用户私网媒体流 RTP/RTCP 地址/端口；并且，将呼叫信令的报文 IP 头地址/端口修改为 PROXY SERVER30 为该呼叫分配的在公网中的呼叫信令地址/端口，将该报文负载中的呼叫信令地址修改为 PROXY SERVER30 为该呼叫分配的在公网中的呼叫信令地址/端口，将该报文负载中的 RTP/RTCP 地址/端口修改为 PROXY SERVER30 为该媒体流分配的在公网中的地址/端口。然后将呼叫信令发送到 SoftX40、41。

当 PROXY SERVER30 收到发向分组用户终端 10 的呼叫信令时，对将该呼叫信令的报文 IP 头地址/端口修改为被记录的呼叫信令的报文 IP 头地址/端口；将该报文负载中呼叫信令地址/端口修改为被记录的呼叫信令地址/端口；将该呼叫信令所携带的 RTP/RTCP 地址/端口，修改为被记录的媒体流 RTP/RTCP 地址/端口；最后按照修改后的呼叫信令报文 IP 头地址对该报文进行转发。

这样呼叫信令以及媒体流就可以通过 PROXY SERVER30 在主被叫之间进行中转。

熟悉本发明领域的技术人员会理解，PROXY SERVER30 可以配置多个 IP 地址对。如果 PROXY SERVER30 上配置有多个私网 IP 地址或多个公网 IP 地址，则可以用一台设备同时实现对多个企业网/驻地网出口 FW/NAT 的穿越或同时代理多个软交换。通过这种方式确保了 PROXY SERVER30 无论在哪种组网模式，无论 NAT 是否对称 NAT，媒体流都能得到正确转发。

此外，通过对信令的处理和分析，PROXY SERVER30 不仅得到本次会话的地址变换情况，还获得了带宽需求等服务质量（Quality of Service，简称“QoS”）信息。由此，它能通过会话状态信息来控制媒体流的通过与关闭，起到网络保护，防范带宽盗用等。PROXY SERVER30 可以提供对用户的接入控制功能、带宽管理功能，提供对媒体流的 QoS 标记、虚拟局域网（Virtual Local Area Network，简称“VLAN”）标记和信息加密。

为了防止 NAT 映射表老化问题，本发明引入了 NAT 地址绑定关系的定时刷新机制，即 PROXY SERVER30 在信令解析获得地址后就主动定期向分组用户终端 10 发起报文，来刷新企业出口 NAT/FW20 上的信令地址映射关系。在解决信令地址对企业出口 NAT 的穿越后，对于媒体流的交互，PROXY SERVER30 采用首包刷新方式来更新媒体流的会话表项或地址转换关系表项，即在终端发出媒体后，经过企业出口的 NAT/FW20 进行转换到达 PROXY SERVER30，通过首包学习得到出口 NAT/FW20 上动态分配的地址/端口信息，从而更新媒体流会话表项，建立一个完整的媒体流会话表项，完成位于公网接入多个企业时的媒体转发功能。

在系统中引入 PROXY SERVER30 后，由于主叫用户和被叫用户的媒体流都经过 PROXY SERVER30，所以 PROXY SERVER30 可以准确地获得媒体流量，从而实现基于报文流量的计费，而不仅仅是传统的基于时长的计费。

SoftX40、41 是软交换设备，作为 NGN 的网络控制层的关键构件，用于提供综合业务和呼叫控制。在收到发送给私网中分组用户终端的信令时转发给 PROXY SERVER30。

下面再具体说明本发明中的基于 FULL PROXY 方式的穿越 NAT/FW 的方法流程。

作为本发明的一个较佳实施例，假设由分组用户终端 10 发起相关业务到分组用户终端 11，过程如图 3 所示：

首先，在步骤 200 中，私网内的分组用户终端 10 向 PROXY SERVER30 发送呼叫信令。分组用户终端 10 将 PROXY SERVER30 看作是软交换设备，该呼叫信令中包含注册和呼叫信息。具体地说，源自分组用户终端 10 的报文先被发送到 NAT/FW20，NAT/FW20 为该呼叫分配一个公网地址/端口，把报文 IP 头的源地址从私网地址/端口修改为分配的公网地址/端口，但是对报文内部的信息不作任何改动，记录下上述私网地址/端口和公网地址/端口的对应关系，然后把该报文转发到 PROXY SERVER30。

然后进入步骤 210，PROXY SERVER30 在收到呼叫信令后，对呼叫信令的报文负载中携带的信息进行解析与处理，记录呼叫信令的报文 IP 头地址/端口，记录报文负载中的呼叫信令地址/端口，记录用户私网媒体流 RTP/RTCP 地址/端口；并且，将呼叫信令的报文 IP 头地址/端口修改为 PROXY SERVER30 为该呼叫分配的在公网中的呼叫信令地址/端口，将该报文负载中的呼叫信令地址修改为 PROXY SERVER30 为该呼叫分配的在公网中的呼叫信令地址/端口，将该报文负载中的 RTP/RTCP 地址/端口修改为 PROXY SERVER30 为该媒体流分配的在公网中的地址/端口。

在 PROXY SERVER30 的信令处理后，进入步骤 220，将信息转发给真正的软交换设备 SoftX40。

接着进入步骤 230，SoftX40 向 PROXY SERVER30 发送回应信令报文。当 SoftX40 收到需要发向分组用户终端 10 的回应信令报文时，转发给 PROXY SERVER30。

此后进入步骤 240，PROXY SERVER30 收到发向私网内分组用户终端 10 的回应信令时，对该回应信令的报文负载信息进行解析，将该报文负载中回应信令地址/端口修改为被记录的呼叫信令地址/端口，将该回应信令所携带的媒体流 RTP/RTCP 地址/端口，修改为被记录的媒体流 RTP/RTCP 地址/端口。通过在步骤 210 和步骤 240 中对报文负载中信令和 RTP/RTCP 地址/

端口的记录和修改，实现了对 NAT/FW 的穿越，并且在任何组网形式下实现穿越时均不需要对现有的 NAT/FW 和用户终端进行改造。

此后进入步骤 250，PROXY SERVER30 将修改后的回应信令发向私网内分组用户终端 10。具体地说，PROXY SERVER30 首先将报文（其中包含修改后的回应信令）发送给 NAT/FW20，该报文的目的地址是 NAT/FW20 为来自分组用户终端 10 的呼叫分配的公网地址/端口，NAT/FW20 从记录的私网地址/端口和公网地址/端口的对应关系表中查询出该报文的公网目的地址/端口所对应的私网地址/端口，然后用查询到的私网地址/端口替换掉该报文的公网目的地址/端口，然后转发给分组用户终端 10。

需要指出的是，上述实施例中提到的私网和公网只是一个具体的特例，实质上只要是两个网络都可以，其中一个网络在 NAT/FW 之内（对应于上述实施例中的私网），另一个网络在 NAT/FW 之外（对应于上述实施例中的公网）。

虽然通过参照本发明的某些优选实施例，已经对本发明进行了图示和描述，但本领域的普通技术人员应该明白，可以在形式上和细节上对其作各种各样的改变，而不偏离所附权利要求书所限定的本发明的精神和范围。

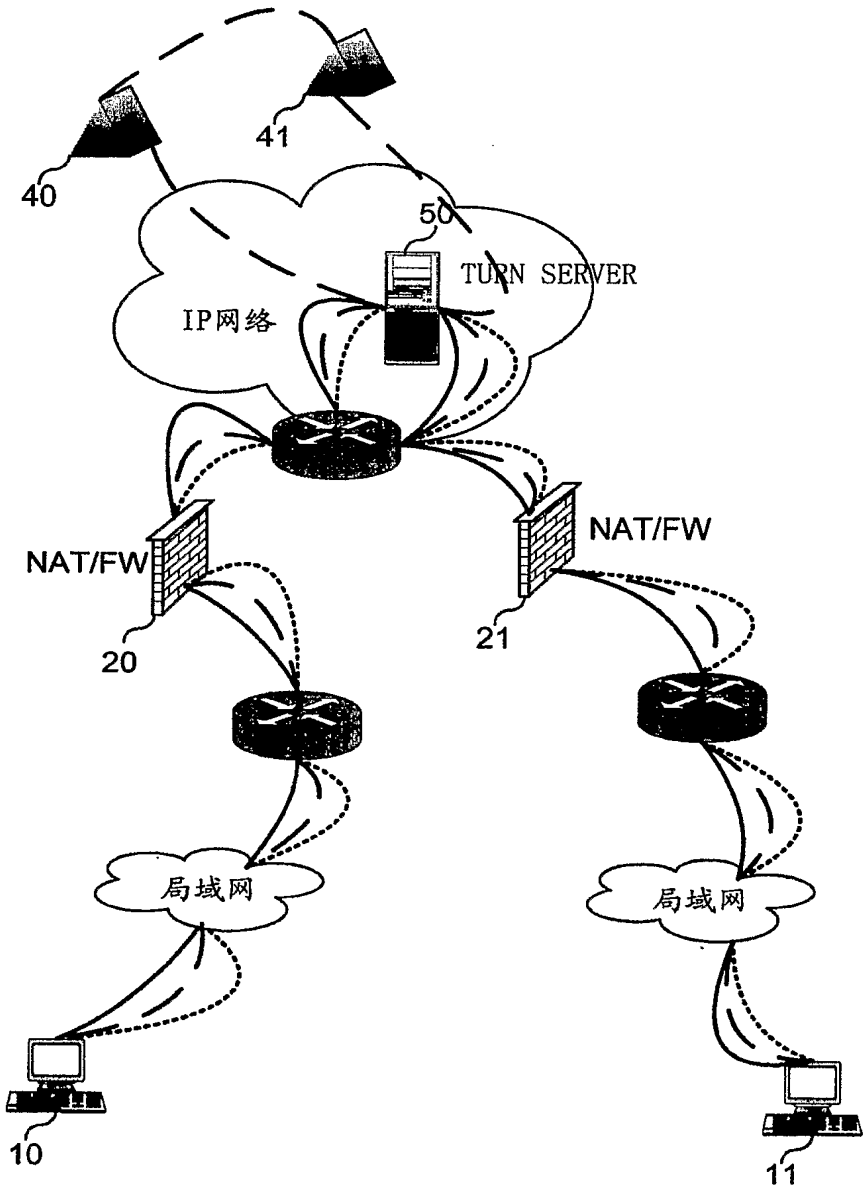


图 1

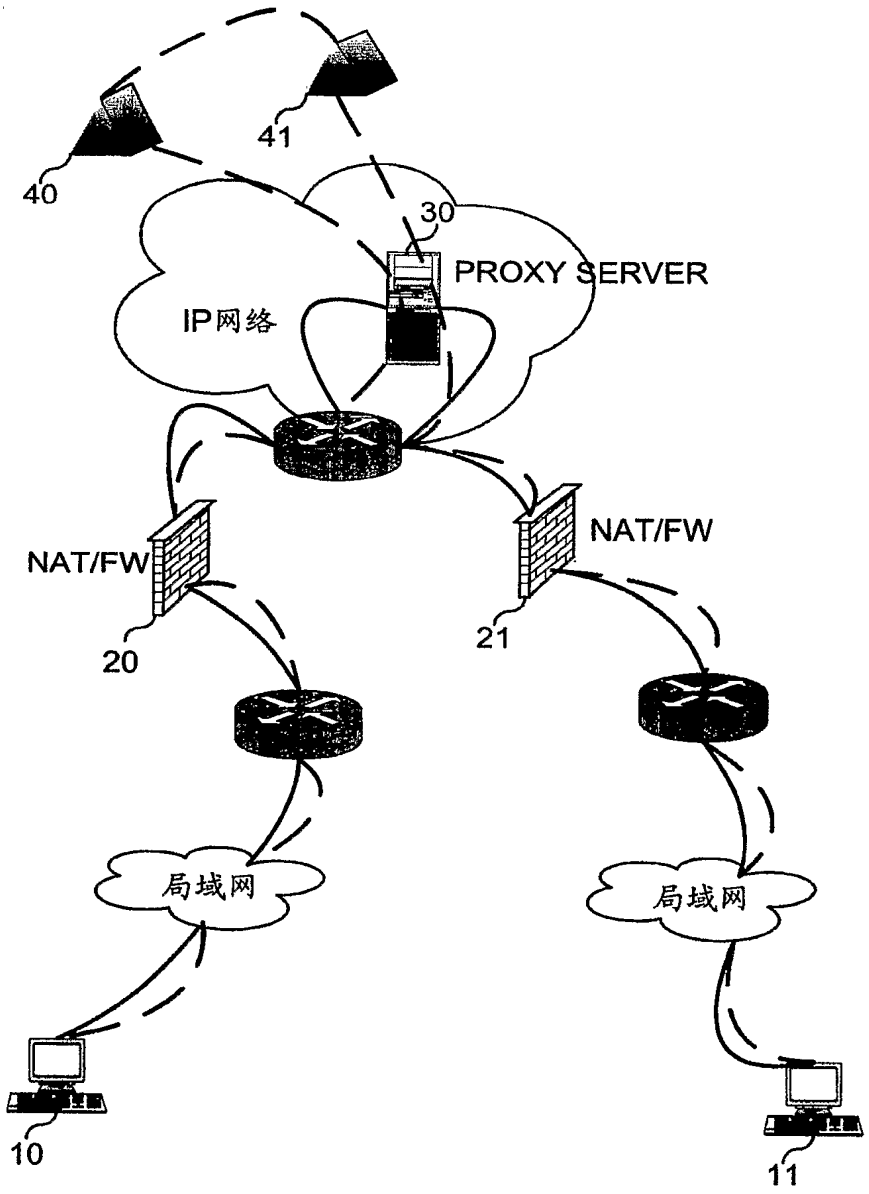


图 2

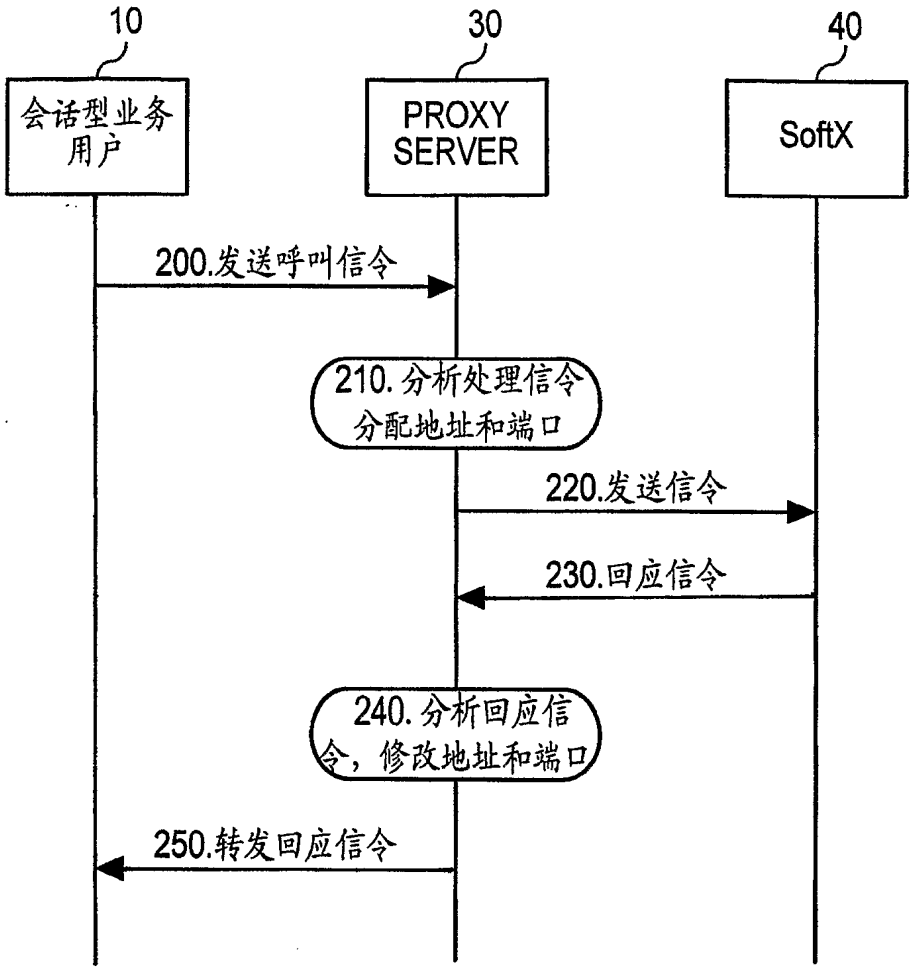

10
30
40
会话型业务用户
PROXY SERVER
SoftX
200.发送呼叫信令
210.分析处理信令分配地址和端口
220.发送信令
230.回应信令
240.分析回应信令，修改地址和端口
250.转发回应信令

图 3